Finding periodic solutions without finding eigenvalues

Autor(en): **Kennedy, Benjamin B.**

Objekttyp: **Article**

Zeitschrift: **Elemente der Mathematik**

Band (Jahr): **73 (2018)**

Heft 1

PDF erstellt am: **25.05.2024**

Persistenter Link: https://doi.org/10.5169/seals-760273

Elem. Math. 73 (2018) 1 – 14
0013-6018/18/010001-14
DOI 10.4171/EM/344

Elemente der Mathematik

Finding periodic solutions without finding eigenvalues

Benjamin B. Kennedy

Benjamin Kennedy received his Ph.D from Rutgers University (USA) in 2007. He is now Associate Professor of Mathematics at Gettysburg College (USA). Professor Kennedy's primary research focus is dynamical systems.

1 Introduction

The nth-order linear scalar-valued difference equation

$$\begin{aligned} x(k) = a_1 x(k-1) + a_2 x(k-2) + \cdots + a_n x(k-n),& \\ n \in \mathbb{Z}_{>0},\quad a_i \in \mathbb{C},\quad x(\cdot) \in \mathbb{C}& \end{aligned} \tag{1}$$

is a staple of introductory dynamical systems courses. A *solution* of Equation (1) is any complex-valued sequence $x = (x(1), x(2), x(3), \ldots)$ such that $x(k)$ obeys the above relationship for all $k \in \mathbb{Z}_{\geq n+1}$. (The first n terms of the sequence are unrestricted and together constitute the *initial condition* of the solution; x is called the continuation of the initial condition as a solution of Equation (1).)

In the study of Equation (1), it is usual to assume that the highest-indexed coefficient a_n is nonzero. Since, however, we shall later be explicitly considering instances of Equation (1) where this is not the case, we do not make the usual assumption that $a_n \neq 0$ here.

Given Equation (1) – that is, given a choice of n and the coefficients a_i – the fundamental question we ask is how solutions can behave as $k \to \infty$. One particular sub-question is

Bei einer skalaren Differenzengleichung der Ordnung n ist man, ähnlich wie bei einer Differentialgleichung, interessiert am Verhalten von Lösungen. Von besonderem Interesse sind dabei periodische Lösungen. Üblicherweise verwandelt man dazu die gegebene Gleichung in ein System von Differenzengleichungen 1. Ordnung. Hat die zugehörige Koeffizientenmatrix eine Einheitswurzel als Eigenwert, so liegt eine periodische Lösung vor. Sogar bei kleinem n ist die entsprechende Rechnung aber recht aufwändig. Der Autor der vorliegenden Arbeit präsentiert nun bei Gleichungen mit rationalen Koeffizienten einen alternativen Weg für das Auffinden periodischer Lösungen, der sogar von Hand leicht zu bewältigen ist.

whether there are nontrivial *r-periodic solutions*: solutions x such that $x(k+r) = x(k)$ for all $k \in \mathbb{Z}_{>0}$, where r is a positive integer.

If x is a periodic solution, we say that $r \in \mathbb{Z}_{>0}$ is the *minimal* period of x if x is not a j-periodic solution for any $j \in \{1, \ldots, r-1\}$. If x has period r but not minimal period r, then the minimal period of x is some divisor of r; therefore finding all r-periodic solutions is the same as finding all j-periodic solutions, where j runs over the divisors of r. Observe that the zero sequence is always a 1-periodic solution for Equation (1).

We usually recast Equation (1) as a matrix equation

$$X(k+1) = AX(k), \quad k \in \mathbb{Z}_{\geq 0}, \tag{2}$$

where

$$A = \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_{n-1} & a_n \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{pmatrix} \quad \text{and} \quad X(k) = \begin{pmatrix} x(n+k) \\ x(n-1+k) \\ \cdots \\ \cdots \\ x(1+k) \end{pmatrix}. \tag{3}$$

With the above notation,

$$X(k+j) = A^j X(k)$$

for any $j \in \mathbb{Z}_{\geq 0}$. The theory of the linear difference equation (2) (with A a general $n \times n$ matrix) is highly developed; see, for example, [3].

Suppose that the point $Y \in \mathbb{C}^n$ is an initial condition for a solution $x = (x_1, x_2, \ldots)$ of Equation (1). With the above notation, this means that

$$Y = (Y_1, \ldots, Y_n)^T = (x_n, \ldots, x_1)^T$$

(note the reversal in the orders of the indices) and that $A^k Y = (x_{n+k}, \ldots, x_{1+k})^T$. If x is r-periodic, we call Y an *r-periodic point* for Equation (2) (and for Equation (1)).

If Y is a nonzero r-periodic point for Equation (2), then

$$Y = A^r Y$$

(here and for the rest of the paper, the matrix A is as in (3)); it follows that 1 is an eigenvalue of A^r with corresponding eigenvector Y. Thus A has at least one eigenvalue that is an rth root of unity; moreover, Y is in the span of all of the eigenvectors corresponding to such eigenvalues. Accordingly, in introductory dynamical systems courses we learn to look for r-periodic solutions of Equation (1) by checking whether any eigenvalues of A are rth roots of unity, and finding the corresponding eigenspaces. As readers who have done this know, carrying out such computations by hand can be laborious, even when n is quite small.

In this paper we present a different approach to finding the periodic solutions of Equation (1) when the coefficients a_i are all rational. If n is small and we are looking for solutions of a particular period r, the method is gratifyingly easy to carry out by hand: it amounts to checking a small list of potential eigen*vectors* rather than potential eigen*values*, and the list depends only on n and r. Indeed, our work shows that the structure of the set of periodic solutions of Equation (1) is – in the rational coefficient case – considerably more rigid than one might first suppose.

We close this section by giving three propositions that follow from our main theorem (Theorem 4.4) and illustrate its flavor. We prove these propositions in Section 4.

Proposition 1.1. *Suppose that a, b, c are rational. The third-order equation*

$$x(k) = ax(k-1) + bx(k-2) + cx(k-3)$$

has nontrivial periodic solutions if and only if at least one of the following holds:

- $(1,1,1)^T \in \mathbb{C}^3$ *is a* 1*-periodic point;*
- $(1,-1,1)^T \in \mathbb{C}^3$ *is a* 2*-periodic point;*
- $(0,1,-1)^T \in \mathbb{C}^3$ *is a* 3*-periodic point;*
- $(0,1,0)^T \in \mathbb{C}^3$ *is a* 4*-periodic point;*
- $(0,1,1)^T \in \mathbb{C}^3$ *is a* 6*-periodic point.*

Proposition 1.2. *Suppose that Equation* (1) *has rational coefficients, and that n is prime and greater than two. Then Equation* (1) *has a periodic solution of minimal period n if and only if*

$$(0,1,-1,1,\ldots,(-1)^n)^T \in \mathbb{C}^n$$

is an n-periodic point for Equation (1)*.*

Proposition 1.3. *Suppose that Equation* (1) *has rational coefficients, and that r is prime. Then if $r > n+1$, Equation* (1) *has no solution of minimal period r.*

Observe that nothing like these results is true without some restriction on the coefficients. For example, given any n and r, we can construct examples of Equation (1) with order n and solutions of minimal period r: we can take ζ to be a primitive rth root of unity and take as our equation

$$x(k) = \zeta^n x(k-n);$$

in this case $(1, \zeta, \ldots, \zeta^{n-2}, \zeta^{n-1}, \zeta^n, \zeta^{n+1}, \ldots)$ is a solution with minimal period r.

2 Algebraic preliminaries

Given the field $F \subseteq \mathbb{C}$, we shall write $F[x]$ for the ring of polynomials in x with coefficients in F, equipped with the usual operations of polynomial addition and multiplication. A polynomial $p(x) \in F[x]$ is called *monic* if the coefficient of its highest-degree term is 1. A polynomial $p(x) \in F[x]$ of positive degree is called *irreducible* if it cannot be expressed as the product of two polynomials of positive degree. We say that $p(x)$ *divides* $f(x)$ if $f(x) = p(x)g(x)$ for some polynomial $g(x)$. Observe that, if $p(x)$ and $f(x)$ are both monic and $p(x)$ divides $f(x)$, then either $p(x) = f(x)$ or the degree of $p(x)$ is strictly smaller than the degree of $f(x)$.

We shall use the following two elementary facts about the ring $F[x]$ (see, for example, [4], Chapters 16 and 17).

- Division algorithm: given polynomials $p(x), a(x) \in F[x]$ with $a(x) \neq 0$, there are unique polynomials $b(x), r(x) \in F[x]$ such that
  i) $p(x) = b(x)a(x) + r(x)$, and
  ii) either $\deg r(x) < \deg a(x)$ or $r(x) = 0$.
- Euclid's Lemma: Suppose that $p(x) \in F[x]$ is irreducible. If $p(x)$ divides $a(x)b(x)$, then $p(x)$ divides either $a(x)$ or $b(x)$.

Suppose now that V is an N-dimensional vector space over the field F, and let $\psi : V \to V$ be a fixed linear transformation. Given the polynomial

$$g(x) = \sum_{i=0}^{d} c_i x^i \in F[x],$$

we define the linear transformation $g(\psi) : V \to V$ by

$$g(\psi) = \sum_{i=0}^{d} c_i \psi^i.$$

We shall need the following well-known fact.

Lemma 2.1. *Let ψ be as above, and suppose that $f(x)$ and $g(x)$ belong to $F[x]$. Then if $h(x) = f(x) + g(x)$ and $k(x) = f(x)g(x)$, we have*

$$h(\psi) = f(\psi) + g(\psi) \quad \textit{and} \quad k(\psi) = f(\psi) \circ g(\psi).$$

Proof. The lemma can be regarded as a consequence of the standard result that the "scalar multiplication"

$$F[x] \times V \ni (g(x), v) \mapsto g(\psi)v$$

makes V into a module over the ring $F[x]$. To see the lemma more directly, we reason as follows.

Write $\mathcal{L}(V)$ for the set of linear transformations on V. The set $\mathcal{L}(V)$ is a ring under the operations of addition and composition. The map $s : F \to \mathcal{L}(V)$ given by $s(a) = aI$ (where I is the identity transformation) is a ring homomorphism. According to the so-called substitution principle (see, for example, Proposition 10.3.4 in [1]), there is a unique ring homomorphism $\bar{s} : F[x] \to \mathcal{L}(V)$ that agrees with s on constant polynomials (i.e., sends the polynomial ax^0 to aI) and that sends x to ψ. The image of $g(x)$ under $\bar{s}$ is just $g(\psi)$, and the statements in the lemma together amount to the assertion that $\bar{s}$ is a ring homomorphism. □

Since the polynomials $f(x)g(x)$ and $g(x)f(x)$ are equal, an important consequence of the second part of the above lemma is that the linear transformations $f(\psi)$ and $g(\psi)$ commute with one another.

Given a vector space V and subspaces $W_1, \dots, W_m$ of V, recall that we say that V is the *direct sum* of the subspaces W_i if every $v \in V$ has a unique expression of the form $w_1 + \cdots + w_m$, where $w_i \in W_i$. Note that, in this case, any two of the subspaces W_i intersect only in the zero vector, and that $\dim V = \sum_i \dim W_i$.

Given the linear transformation $\psi : V \to V$, we say that the subspace $W \subseteq V$ is *ψ-invariant* if $\psi(W) \subseteq W$.

The *minimal polynomial* of ψ is the unique monic polynomial $q(x)$ of lowest degree such that $q(\psi)v = 0$ for all $v \in V$. The existence of the minimal polynomial is standard; see, for example, Chapter 7 of [6].

The following is the main theorem underpinning our results.

Proposition 2.2. *Let $N \in \mathbb{Z}_{>0}$. Let V be an N-dimensional vector space over the field F, and let $\psi : V \to V$ be a linear transformation. Let $q(x)$ be the minimal polynomial of ψ. Suppose that $q(x)$ is of degree N and factors in $F[x]$ as*

$$q(x) = p_1(x) \cdots p_m(x),$$

where the $p_i(x)$ are all monic and irreducible, and are all distinct. Then there are m subspaces $W_1, \dots, W_m$ such that the following hold.

(i) *Each subspace W_i is nontrivial and ψ-invariant, and $W_i = \{v \in V \ : \ p_i(\psi)v = 0\}$.*

(ii) *V is the direct sum of the subspaces $W_1, \dots, W_m$.*

(iii) *Given any nonzero $v \in W_i$, the set*

$$\{\ v,\ \psi v,\ \dots\ \psi^{\deg p_i(x) - 1} v\ \}$$

is a basis for W_i.

(iv) *Given any nonzero $v \in W_i$ and $B(x) \in F[x]$, if $B(\psi)v = 0$ then $p_i(x)$ divides $B(x)$.*

(v) *Any ψ-invariant subspace of V is the direct sum of some subset of the W_i.*

(vi) *Given any nonempty subset $S \subseteq \{1, \dots, m\}$ and $P(x) = \prod_{i \in S} p_i(x)$, any ψ-invariant subspace of the kernel of $P(\psi)$ is the direct sum of some subset of the W_i, where $i \in S$.*

Observe that point (v) is actually a special case of (vi) with $P(x)$ equal to $q(x)$, the minimal polynomial of ψ; but we will prove the two cases separately below.

Remark 2.3. It is part (v) of Proposition 2.2 that is especially important for us, and it is not true without our restrictions on the linear transformation ψ. Consider the identity transformation I on F^N, where $N > 1$: the minimal polynomial of I is $q(x) = x - 1$, and so $\deg q(x) < N$. While F^N is certainly expressible as the direct sum of a collection of lower-dimensional identity-invariant subspaces (for example, the subspaces spanned by each standard basis vector) it is not the case that every identity-invariant subspace – i.e., every subspace – is the direct sum of a subset of those subspaces.

Proof of Proposition 2.2. Points (i) and (ii) are part of a standard decomposition theorem for modules over principal ideal domains (see, for example, Theorem 7.8 in [6]).

For (iii), choose a nonzero $v \in W_i$, and consider the vectors

$$v^0 = v, \quad v^1 = \psi v, \quad v^2 = \psi^2 v, \quad \ldots .$$

Since $p_i(\psi)v = 0$, the set $\{v^0, v^1, v^2, \ldots, v^{\deg p_i(x)}\}$ is linearly dependent. Let $s \leq \deg p_i(x)$ be the largest positive integer such that

$$\{v^0, v^1, v^2, \ldots, v^{s-1}\}$$

is linearly independent. There are unique scalars $a_0, \ldots, a_{s-1} \in F$ such that

$$v^s - a_{s-1}v^{s-1} - \cdots - a_0 v^0 = 0.$$

Let us write

$$a(x) = x^s - a_{s-1}x^{s-1} - \cdots - a_0;$$

we have $a(\psi)v = 0$. By the division algorithm we can write

$$p_i(x) = b(x)a(x) + r(x), \quad \text{where } \deg r(x) < \deg a(x) = s \text{ or } r(x) = 0.$$

Applying Lemma 2.1, we have

$$0 = p_i(\psi)v = b(\psi)(a(\psi)v) + r(\psi)v = r(\psi)v.$$

If $r(x) \neq 0$, then $r(\psi)v = 0$ is a nontrivial linear combination of the vectors $\{v^0$, v^1, v^2, …, $v^{\deg r(x)}\}$; since $\deg r(x) < s$ and $\{v^0, v^1, v^2, \ldots, v^{s-1}\}$ is linearly independent, we obtain a contradiction. We conclude that $r(x) = 0$, and that $a(x)$ divides $p_i(x)$. By assumption $p_i(x)$ is irreducible; therefore $a(x) = p_i(x)$ and $s = \deg p_i(x)$. It follows that the vectors described in part (iii) form a linearly independent set, and that $\dim W_i \geq \deg p_i(x)$. Since $\deg q(x) = \sum_i \deg p_i(x) = N = \dim V$, we must actually have $\dim W_i = \deg p_i(x)$ for all i, and so the set of vectors described in part (iii) is a basis for W_i. This proves part (iii).

Suppose that $v \in W_i$ is nonzero and that $B(\psi)v = 0$. Again by the division algorithm we can write

$$B(x) = b(x)p_i(x) + r(x), \quad \text{where} \quad \deg r(x) < \deg p_i(x) \text{ or } r(x) = 0.$$

Similarly as in the last part we use Lemma 2.1 to conclude that $r(\psi)v = 0$. If $r(x) \neq 0$, this implies that the set $\{v^0, v^1, v^2, \ldots, v^{\deg r(x)}\}$ is not linearly independent. Since $\deg r(x) < \deg p_i(x)$, this implies that the set $\{v^0, v^1, \ldots, v^{\deg p_i(x)-1}\}$ is not linearly independent either, contradicting (iii); we must have that $r(x) = 0$, and that $p_i(x)$ divides $B(x)$. This completes the proof of part (iv).

We now prove part (v). If $m = 1$, then part (iii) implies that the only ψ-invariant subspaces are the trivial subspace and $W_1 = V$, since $\{v^0, v^1, \ldots, v^{\deg p_i(x)-1}\}$ is a basis for $W_1 = V$ for any nonzero $v \in V$. Suppose now that $m > 1$. Choose and fix a nonzero $v_i \in W_i$ for each i, and write $v_i^j = \psi^j v_i$, $j \in \{0, \ldots, \deg p_i(x) - 1\}$. Our work so far shows that the vectors v_i^j constitute a basis for V. Suppose that W is a ψ-invariant subspace. Given any $v \in W$, we can express v uniquely as a linear combination of the basis vectors v_i^j:

$$v = a_1^0 v_1^0 + \cdots + a_i^j v_i^j + \cdots + a_m^{\deg p_m(x)-1} v_m^{\deg p_m(x)-1}, \quad a_i^j \in F.$$

Suppose that, in the above sum, $a_i^j \neq 0$. Define

$$R_i(x) = p_1(x)p_2(x)\cdots p_{i-1}(x)p_{i+1}(x)\cdots p_m(x).$$

We now make the following observations.

- Since W is ψ-invariant, $R_i(\psi)v \in W$.
- Lemma 2.1 and part (i) show that $R_i(\psi)w = 0$ for any $w \in W_\ell$, where $\ell \neq i$.
- The invariance of W_i implies that $R_i(\psi)w \in W_i$ for any $w \in W_i$.
- By repeated application of Euclid's Lemma we see that $p_i(x)$ does not divide $R_i(x)$; (the contrapositive of) part (iv) now implies that $R_i(\psi)w \neq 0$ for any nonzero $w \in W_i$.

By the above observations and the linearity of $R_i(\psi)$, we conclude that $R_i(\psi)v$ is an element of $W \cap W_i$ and is nonzero. Again since W is ψ-invariant, it follows from part (iii) that W contains a basis for W_i, and hence contains all of W_i.

We have shown that W either contains W_i or, in the notation above, that $a_i^j = 0$ for all $v \in W$ and all $1 \leq j \leq \deg p_i(x) - 1$; otherwise put, W either contains W_i or is contained in the direct sum of the subspaces W_ℓ, $\ell \neq i$. We conclude that W is the direct sum of the subspaces W_i it contains.

Finally, we prove part (vi). Suppose that W is a ψ-invariant subspace of $\ker P(\psi)$. We know from part (v) that W is a direct sum of some subset of the W_i. Suppose that $u_i \in W \cap W_i \setminus \{0\}$. Then by part (iv) we have that $p_i(x)|P(x)$, and repeated application of Euclid's lemma now yields that $i \in S$. This completes the proof. □

We shall also need the following linear algebra lemma.

Lemma 2.4. *Suppose that $F \subseteq \mathbb{C}$ is a field, and that M is an $N \times N$ matrix with entries in F. Let $\lambda \in F$ be an eigenvalue of M. Write E for the corresponding eigenspace in $\mathbb{C}^N$, and write $\tilde{E}$ for the corresponding eigenspace in F^N. Then E and $\tilde{E}$ have the same dimension, and any basis for $\tilde{E}$ is also a basis for E.*

Proof. If B is any $n \times m$ matrix with entries in F, the rank and nullity of B are the same whether we regard B as an element of $\mathrm{Mat}_{n\times m}(F)$ or as an element of $\mathrm{Mat}_{n\times m}(\mathbb{C})$ (see, for example, Theorem 6.4.35 and the subsequent discussion in [5], or Problem 7.2.1 in [2]).

We write I for the identity matrix. The dimension of E is the nullity of $M - \lambda I$ where $M - \lambda I$ is viewed as an element of $\mathrm{Mat}_{N\times N}(\mathbb{C})$; the dimension of $\tilde{E}$ is the nullity of $M - \lambda I$ where $M - \lambda I$ is viewed as an element of $\mathrm{Mat}_{N\times N}(F)$. By the observation of the last paragraph, E and $\tilde{E}$ have the same dimension; call it D. It is therefore enough to prove that a basis of $\tilde{E}$ is linearly independent when viewed as a subset of $\mathbb{C}^N$; but again, the matrix whose columns are the members of a basis of $\tilde{E}$ has the same rank whether regarded as an element of $\mathrm{Mat}_{N\times D}(F)$ or as an element of $\mathrm{Mat}_{N\times D}(\mathbb{C})$. □

3 The space $\mathbf{Per}_r(A)$

We define the *shift operator* $S_n : \mathbb{C}^n \to \mathbb{C}^n$ by

$$S_n(x_1, x_2, \dots, x_n)^T = (x_n, x_1, \dots, x_{n-1})^T.$$

We also write I for the identity transformation.

Lemma 3.1. *Let $F \subseteq \mathbb{C}$ be a field. The minimal polynomial of S_n in F^n is $x^n - 1$.*

Proof. It is clear that $(S_n^n - I)v = 0$ for all $v \in F^n$. On the other hand, if

$$g(x) = \sum_{i=0}^{n-1} b_i x^i$$

is any nonzero polynomial in $F[x]$ of degree less than n and e_n is the nth standard basis vector in F^n, we see that

$$g(S_n)e_n = (b_1, b_2, \dots, b_{n-1}, b_0)^T \neq 0,$$

and so $g(x)$ is not the minimal polynomial of S_n. □

We henceforth write $Q_n(x) = x^n - 1$.

Given $d \in \mathbb{Z}_{>0}$, we write $\Phi_d(x)$ for the so-called *dth cyclotomic polynomial*. We write $\phi : \mathbb{Z}_{>0} \to \mathbb{Z}_{>0}$ for the Euler totient function, defined as follows: $\phi(1) = 1$; and for $d > 1$, $\phi(d)$ is the number of positive integers that are both less than d and relatively prime to d. The following proposition is standard (see, for example, [4], Chapters 17 and 33):

Proposition 3.2. *For each $n \in \mathbb{Z}_{>0}$,*

$$Q_n(x) = \prod_{d|n} \Phi_d(x).$$

Each cyclotomic polynomial $\Phi_d(x)$ is monic, has integer coefficients, is of degree $\phi(d)$, and is irreducible in $\mathbb{Q}[x]$. The cyclotomic polynomials $\Phi_d(x)$ are all distinct. □

Given $d \in \mathbb{Z}_{>0}$, let us choose and fix a nonzero vector $u[d] \in \mathbb{Q}^d$ such that

$$\Phi_d(S_d)u[d] = 0.$$

For example, since $\Phi_3(x) = x^2 + x + 1$ we require $u[3]$ to be a three-dimensional rational vector such that

$$\Phi_3(S_3)u[3] = (S_3^2 + S_3 + I)u[3] = 0;$$

we may take $u[3] = (0, 1, -1)^T$. Similarly, since $\Phi_4(x) = x^2 + 1$ we require $u[4]$ to be a four-dimensional rational vector such that

$$\Phi_4(S_4)u[4] = (S^2 + I)u[4] = 0;$$

we may take $u[4] = (0, 1, 0, -1)^T$.

Given $u[d]$, let us define $\sigma[d]$ to be the set

$$\sigma[d] = \{\, u[d], S_d u[d], \dots, S_d^{\phi(d)-1} u[d] \,\} \subseteq \mathbb{Q}^d.$$

Proposition 2.2, applied to the vector space $\mathbb{Q}^d$ and the linear transformation $S_d : \mathbb{Q}^d \to \mathbb{Q}^d$, shows that $\sigma[d]$ is a linearly independent subset of $\mathbb{Q}^d$ (since $\Phi_d(x)$ is an irreducible factor in $\mathbb{Q}[x]$ of the minimal polynomial $Q_d(x)$ of S_d).

Given $d \in \mathbb{Z}_{>0}$ and $n \in \mathbb{Z}_{>0}$, we define the linear transformation $\tau_d^n : \mathbb{C}^d \to \mathbb{C}^n$ as follows. If $d > n$, $\tau_d^n v$ is the truncation of v to its first n entries:

$$\tau_d^n (v_1, \dots, v_d)^T = (v_1, \dots, v_n)^T.$$

If $d = n$, $\tau_d^n v = v$. If $n > d$, then $\tau_d^n v$ is the vector obtained by extending the entries of v d-periodically:

$$\tau_d^n (v_1, \dots, v_d)^T = (v_1, \dots, v_d, \dots, v_n)^T, \quad v_j = v_i \text{ if } |i - j| = d.$$

We shall need the following simple observation.

Lemma 3.3. *Given $N, n, d \in \mathbb{Z}_{>0}$ with $N \geq n$, $\tau_N^n \circ \tau_d^N = \tau_d^n$.* □

Lemma 3.4. *Let $w \in \mathbb{Q}^d$, where $d|n$. For any polynomial $f(x) \in \mathbb{Q}[x]$ we have*

$$\tau_d^n (f(S_d) w) = f(S_n)(\tau_d^n w).$$

Proof. By linearity, it is enough to prove the lemma for $f(x) = x^p$, $p \in \mathbb{Z}_{\geq 0}$. The $p = 0$ case is obvious, since in this case $f(S_n) = I$. For the $p = 1$ case, we compute (recalling that d divides n)

$$\tau_d^n S_d w = \tau_d^n (w_d, w_1, \dots, w_{d-1})^T = (w_d, w_1, \dots, w_{d-1}, w_d, \dots, w_{d-1})^T$$

(this is n/d concatenated copies of $S_d w$), and

$$S_n \tau_d^n w = S_n (w_1, \dots, w_d, w_1, \dots, w_d)^T = (w_d, w_1, \dots, w_{d-1}, w_d, \dots, w_{d-1})^T$$

(this is also n/d concatenated copies of $S_d w$). Assume the formula holds for $p \leq P$. Then applying the formula for $p = P$ and $p = 1$ in turn we get

$$\tau_d^n S_d^{P+1} w = \tau_d^n S_d^P S_d w = S_n^P \tau_d^n S_d w = S_n^P S_n \tau_d^n w = S_n^{P+1} \tau_d^n w;$$

the desired result follows by induction. □

We now return to Equation (2). Recall that we are writing $A \in \mathrm{Mat}_{n \times n}(\mathbb{C})$ for the matrix associated with Equation (2) – its form is given in (3).

Let us write $\mathrm{Per}(A) \subseteq \mathbb{C}^n$ for the set of periodic points of Equation (2), and $\mathrm{Per}_r(A) \subseteq \mathbb{C}^n$ for the set of periodic points of Equation (2) with (not necessarily minimal!) period r. The following lemma is clear.

Lemma 3.5. *The sets* $\mathrm{Per}(A)$ *and* $\mathrm{Per}_r(A)$ *are linear subspaces of* $\mathbb{C}^n$ *and are* A*-invariant:* $Av \in \mathrm{Per}(A)$ *if* $v \in \mathrm{Per}(A)$*, and* $Av \in \mathrm{Per}_r(A)$ *if* $v \in \mathrm{Per}_r(A)$. □

We are interested in describing a basis for the subspace $\mathrm{Per}_r(A) \subseteq \mathbb{C}^n$ in the case that A has rational entries. The subspace $\mathrm{Per}_r(A)$ is precisely the eigenspace in $\mathbb{C}^n$ of A^r corresponding to the eigenvalue 1.

Now consider Equation (2) *in the setting of the vector space* $\mathbb{Q}^n$ (rather than $\mathbb{C}^n$). Write $\mathrm{Per}_r^{\mathbb{Q}}(A)$ for the subspace of r-periodic points of Equation (2), viewed as an equation in $\mathbb{Q}^n$. $\mathrm{Per}_r^{\mathbb{Q}}(A)$ is precisely the eigenspace in $\mathbb{Q}^n$ of A^r corresponding to the eigenvalue 1. By Lemma 2.4, $\mathrm{Per}_r^{\mathbb{Q}}(A)$ and $\mathrm{Per}_r(A)$ have the same dimension, and any basis of $\mathrm{Per}_r^{\mathbb{Q}}(A) \subseteq \mathbb{Q}^n$ serves as a basis of $\mathrm{Per}_r(A) \subseteq \mathbb{C}^n$. We will now use the work of Section 2 to describe a basis of $\mathrm{Per}_r^{\mathbb{Q}}(A)$ in the case that $r|n$. This description undergirds our main theorems.

The crucial observation is the following. If $v \in \mathrm{Per}_r^{\mathbb{Q}}(A)$, then the entries of v are r-periodic in the sense that $v_k = v_j$ if $|k-j| = r$. If we moreover have $r|n$, then the first entry of Av will be equal to the nth entry of v – and so $Av = S_n v$. Since $Av \in \mathrm{Per}_r^{\mathbb{Q}}(A)$ by Lemma 3.5, we conclude that $\mathrm{Per}_r^{\mathbb{Q}}(A)$ is S_n-invariant. Furthermore, applying the above observation r times yields $A^r v = S_n^r v = v$. We have established the following lemma.

Lemma 3.6. *Given* $r|n$*, the subspace* $\mathrm{Per}_r^{\mathbb{Q}}(A)$ *is* S_n*-invariant. Furthermore,* $\mathrm{Per}_r^{\mathbb{Q}}(A)$ *is contained in the kernel of* $S_n^r - I = Q_r(S_n)$. □

We now apply Proposition 2.2 to describe the S_n-invariant subspaces of $\mathbb{Q}^n$ (of which $\mathrm{Per}_r^{\mathbb{Q}}(A)$ is one when $r|n$, as we have just observed). Let us assume that n has m distinct positive divisors $1 = d_1 < \cdots < d_m = n$. Proposition 3.2 and Proposition 2.2 now yield the following. The space $\mathbb{Q}^n$ is equal to the direct sum of m nontrivial S_n-invariant subspaces

$$V_1, \ldots, V_m,$$

where V_i has dimension $\phi(d_i)$. Any vector v in V_i satisfies $\Phi_{d_i}(S_n)v = 0$. Conversely, if $v \in \mathbb{Q}^n$ is nonzero and satisfies $\Phi_{d_i}(S_n)v = 0$, then $\{v, S_n v, \ldots, S_n^{\phi(d_i)-1}v\}$ is a basis for V_i. Any S_n-invariant subspace of $\mathbb{Q}^n$ is the direct sum of some subset of the subspaces V_i. Finally, given $r|n$, any S_n-invariant subspace that also lies in the kernel of

$$S_n^r - I = Q_r(S_n) = \prod_{j|r} \Phi_j(S_n)$$

is a direct sum of some subset of the subspaces V_j for which $j|r$.

What this means is that, if we can find a nonzero vector $v_i \in V_i$ for every $i \in \{1, \ldots, m\}$, then any S_n-invariant subspace (in particular, any of the subspaces $\mathrm{Per}_r^{\mathbb{Q}}(A)$, where $r|n$) is determined, completely, by which of the vectors v_i lie in that subspace. More particularly, since $\mathrm{Per}_r^{\mathbb{Q}}(A)$ is in the kernel of

$$S_n^r - I = Q_r(S_n) = \prod_{j|r} \Phi_j(S_n),$$

$\mathrm{Per}_r^{\mathbb{Q}}(A)$ is determined, completely, by which of the vectors v_j with $j|r$ lie in $\mathrm{Per}_r^{\mathbb{Q}}(A)$.

Lemma 3.7. *In the notation established above, we can take as a basis for V_i the set*

$$\tau^n_{d_i}\sigma[d_i],$$

where $\sigma[d_i]$ is as described above.

Proof. For notational simplicity, we shall write d_i as d and V_i as V.
By Lemma 3.4 we have that

$$\Phi_d(S_n)\tau^n_d u[d] = \tau^n_d \Phi_d(S_d)u[d] = 0;$$

thus $\tau^n_d u[d] \in V$. Thus by part (iii) of Proposition 2.2 the vectors

$$S^j_n \tau^n_d u[d] = \tau^n_d S^j_d u[d], \quad j \in \{0, \dots, \phi(d) - 1\}$$

form a basis for V – but this is just the set $\tau^n_d \sigma[d]$. □

Lemma 3.7 and part (iv) of Proposition 2.2 show that, given any $r|n$, $\mathrm{Per}^{\mathbb{Q}}_r(A)$ (and hence $\mathrm{Per}_r(A)$) has a basis of the form

$$\bigcup\{\ \tau^n_{d_i}\sigma[d_i]\ :\ d_i|r \text{ and } \tau^n_{d_i}u[d_i] \in \mathrm{Per}^{\mathbb{Q}}_r(A)\ \}.$$

Given Equation (1), then, we can determine a basis for $\mathrm{Per}_r(A)$ simply by checking which vectors $\tau^n_{d_i}u[d_i]$ lie in $\mathrm{Per}_r(A)$, as d_i runs across the divisors of r. Otherwise put, if we write

$$\mathcal{D} = \{d_i \in \mathbb{Z}_{>0}\ :\ d_i|r \text{ and } \tau^n_{d_i}u[d_i] \in \mathrm{Per}_r(A)\}$$

then the disjoint union

$$\bigcup_{d_i \in \mathcal{D}} \tau^n_{d_i}\sigma[d_i]$$

is a basis for $\mathrm{Per}_r(A)$. Observe that $\mathrm{Per}_r(A)$ has dimension $\sum_{d_i \in \mathcal{D}} \phi(d_i)$. (Note carefully that r itself does not necessarily belong to $\mathcal{D}$.)

Suppose that, in the notation above, $\bar{r}$ is the least common multiple of the divisors $d_i \in \mathcal{D}$. Then $\bar{r}|r$, and for each $v \in \mathrm{Per}^{\mathbb{Q}}_r A$ we have that $Q_{\bar{r}}(S_n)v = 0$ (since $\Phi_{d_i}(x)|Q_{\bar{r}}(x)$ for all $d_i \in \mathcal{D}$). This means that each $v \in \mathrm{Per}^{\mathbb{Q}}_r A$ actually lies in $\mathrm{Per}^{\mathbb{Q}}_{\bar{r}} A$ and hence in $\mathrm{Per}_{\bar{r}} A$. If $\bar{r} < r$, then, we conclude that no member of $\mathrm{Per}_r A$ has *minimal* period r. Contrapositively, if there is a point in $\mathrm{Per}_r A$ with minimal period r, we must have that $r = \mathrm{lcm}\{d_i : d_i \in \mathcal{D}\}$.

Summing up the discussion of this section we obtain the following proposition.

Proposition 3.8. *Suppose that Equation* (1) *has rational coefficients, and that $r|n$. Then the following hold. If Equation* (1) *has a nontrivial solution of period r, then* $\mathrm{Per}_r(A)$ *has a basis of the form*

$$\bigcup_{d_i \in \mathcal{D}} \tau^n_{d_i}\sigma[d_i],$$

where

$$\mathcal{D} = \{d_i \in \mathbb{Z}_{>0}\ :\ d_i|r \text{ and } \tau^n_{d_i}u[d_i] \in \mathrm{Per}_r(A)\}.$$

$\mathrm{Per}_r(A)$ *has dimension* $\sum_{d_i \in \mathcal{D}} \phi(d_i)$.

If Equation (1) *has a nontrivial solution of minimal period r, then moreover we have that r is the least common multiple of the members of $\mathcal{D}$.* □

4 The main theorem

Given $N \geq n$, we define the *N-dimensional extension* $(1)_N$ of Equation (1) to be the N-dimensional equation obtained simply by adding an appropriate number of zero coefficients:

$$x(k) = a_1 x(k-1) + a_2 x(k-2) + \cdots + a_N x(k-N),$$
$$a_{n+1} = a_{n+2} = \cdots = a_N = 0.$$

We shall write A_N for the coefficient matrix corresponding to $(1)_N$.

Following the notation used above, we write $\mathrm{Per}_r(A_N)$ for the subspace of r-periodic points of Equation $(1)_N$.

Since $a_{n+1} = \cdots = a_N = 0$, the $(n+1)$st through Nth entries of an initial condition for Equation $(1)_N$ are irrelevant in the sense that they have no effect on the initial condition's continuation; loosely speaking, the initial condition $v \in \mathbb{C}^N$ continues as a solution of Equation $(1)_N$ in the same way as does $\tau_N^n v \in \mathbb{C}^n$ as a solution of Equation (1). More specifically we have the following lemma, whose proof we omit.

Lemma 4.1. *Given any $N \geq n$, a sequence is a periodic solution of Equation* (1) *of* (*minimal*) *period r if and only if it is a periodic solution of Equation* $(1)_N$ *of* (*minimal*) *period r.*

If the continuation of $v \in \mathbb{C}^N$ as a solution of Equation $(1)_N$ *has* (*minimal*) *period r, then the continuation of $\tau_N^n v \in \mathbb{C}^n$ as a solution of Equation* (1) *has* (*minimal*) *period r also.*

If the continuation of $w \in \mathbb{C}^n$ as a solution of Equation (1) *has* (*minimal*) *period r, then there is a unique vector $v \in \mathbb{C}^N$ such that $\tau_N^n v = w$ and the continuation of v as a solution of Equation* $(1)_N$ *has* (*minimal*) *period r also.* □

We now consider Equations (1) and $(1)_N$ together, where $N \geq n$. We shall make frequent use of Lemma 4.1, and of the discussion preceding it.

Lemma 4.2. *Suppose that $N \geq n$ and that $B \subseteq \mathbb{C}^N$ is a basis of* $\mathrm{Per}_r(A_N)$. *Then the set $\tau_N^n B$ is a basis of* $\mathrm{Per}_r(A)$, *and* $\mathrm{Per}_r(A_N)$ *and* $\mathrm{Per}_r(A)$ *have the same dimension.*

Proof. That $\tau_N^n B$ lies in $\mathrm{Per}_r(A)$ is clear from Lemma 4.1. We now show that $\tau_N^n B$ actually spans $\mathrm{Per}_r(A)$ and is a linearly independent set.

Suppose that $w \in \mathrm{Per}_r(A)$. Then by Lemma 4.1 there is a unique vector $v \in \mathrm{Per}_r(A_N)$ such that $\tau_N^n v = w$. Since v is a linear combination of members of B and τ_N^n is merely a truncation operator, w is a linear combination of members of $\tau_N^n B$. Thus $\tau_N^n B$ spans $\mathrm{Per}_r(A)$, and $\dim \mathrm{Per}_r(A) \leq \dim \mathrm{Per}_r(A_N)$.

Write $B = \{v_1, \ldots, v_k\}$. If we imagine that $\sum_i a_i \tau_N^n v_i = 0$ where the a_i are not all zero, then $v = \sum_i a_i v_i \in \mathrm{Per}_r(A_N)$ is equal to zero in its first n entries. Since the continuation of v as a solution of Equation $(1)_N$ is the same as the continuation of $\tau_N^n v$ as a solution of Equation (1), the continuation of v as a solution of Equation $(1)_N$ is eventually zero. Since $v \in \mathrm{Per}_r(A_N)$, though, we must have that v is identically zero – contradicting the linear independence of B. We conclude that $\tau_N^n B$ is a linearly independent set in $\mathbb{C}^n$, and that $\dim \mathrm{Per}_r(A_N) \leq \dim \mathrm{Per}_r(A)$. □

The above lemma yields in particular that

Lemma 4.3. *The dimension of* $\mathrm{Per}_r(A_N)$ *is no greater than* n. □

We are now ready to state our main theorem.

Theorem 4.4. *Suppose that Equation* (1) *has rational coefficients. If Equation* (1) *has a nontrivial solution of period* r*, then* $\mathrm{Per}_r(A)$ *has a basis of the form*

$$\bigcup_{d_i \in \mathcal{D}} \tau^n_{d_i} \sigma[d_i],$$

where

$$\mathcal{D} = \{d_i \in \mathbb{Z}_{>0} \ : \ d_i | r \text{ and } \tau^n_{d_i} u[d_i] \in \mathrm{Per}_r(A)\}.$$

$\mathrm{Per}_r(A)$ *has dimension* $\sum_{d_i \in \mathcal{D}} \phi(d_i)$.
If Equation (1) *has a nontrivial solution of minimal period* r*, then moreover we have that* r *is the least common multiple of the members of* $\mathcal{D}$.

Proof. Choose any $N \geq n$ with $r|N$, and consider the extended equation $(1)_N$. Then by Lemma 4.1, Equation $(1)_N$ has a nontrivial solution of period $r|N$ as well; and if Equation (1) has a nontrivial solution of minimal period r, then Equation $(1)_N$ does as well. Since $\tau^n_N \tau^N_d v = \tau^n_d v$ for any $v \in \mathbb{C}^d$ (Lemma 3.3), the description of the basis of $\mathrm{Per}_r(A)$ and its dimension follows from Proposition 3.8 (applied to Equation $(1)_N$) and Lemma 4.2. □

Now suppose that Equation (1) has rational coefficients and a solution of *minimal* period r. The dimension of $\mathrm{Per}_r(A)$ is no greater than n but is also equal to $\sum_{d_i \in \mathcal{D}} \phi(d_i)$, where $\mathcal{D}$ is some set of positive integers whose least common multiple is r. Thus r cannot be the least common multiple of any set of divisors d_i for which $\sum_{d_i \in \mathcal{D}} \phi(d_i) > n$. Since $\phi(d) \to \infty$ as $d \to \infty$, we see that, given n, there are only finitely many possibilities for r. In particular, given Equation (1), the following choice of N is well defined:

$$N = \mathrm{lcm}(n, \{\ q \ : \ \text{Equation (1) has a solution of minimal period } q\ \}).$$

Note that, with this choice of N, $\mathrm{Per}(A) = \mathrm{Per}_N(A)$. Applying Theorem 4.4 with N in the place of r, then, and using the fact that $\sigma[d]$ has $\phi(d)$ elements, we obtain as a corollary the following description of the basis of the whole space $\mathrm{Per}(A)$ of periodic solutions.

Corollary 4.5. *Suppose that Equation* (1) *has rational coefficients. If* $\mathrm{Per}(A)$ *is nontrivial it has as basis*

$$\bigcup \{\ \tau^n_d \sigma[d] \ : \ \phi(d) \leq n \text{ and } \tau^n_d u[d] \in \mathrm{Per}(A)\ \}.$$ □

Again since $\phi(d) \to \infty$ as $d \to \infty$, this corollary gives us a finite list of potential periodic points of Equation (1) to check to describe all periodic points of Equation (1) (in the case that the coefficients are all rational).

Remark 4.6. Note that, in the above corollary, if we write $\mathcal{D}$ for the set of all d such that $\tau^n_d u[d] \in \mathrm{Per}(A)$, we must actually have $\sum_{d \in \mathcal{D}} \phi(d) \leq n$. In the other direction, given n and a collection of $\mathcal{D}$ of distinct natural numbers such that $\sum_{d \in \mathcal{D}} \phi(d) \leq n$, it can be shown that there is some instance of Equation (1) with rational coefficients such that $\mathrm{Per}(A)$ has precisely $\bigcup_{d \in \mathcal{D}} \tau^n_d \sigma[d]$ as a basis.

We conclude by proving the propositions stated in Section 1.

Proof of Proposition 1.1. The only numbers d with $\phi(d) \leq 3$ are 1, 2, 3, 4, and 6. Thus if Equation (1) has rational coefficients and $n = 3$ we need only check whether $\tau_d^3 u[d]$ are periodic points for $d = 1, 2, 3, 4, 6$. The rest of the proof follows from the observations that the following vectors are valid choices of $u[d]$:

$$u[1] = (1)^T; \quad u[2] = (1, -1)^T; \quad u[3] = (0, 1, -1)^T; \quad u[4] = (0, 1, 0, -1)^T;$$
$$u[6] = (0, 1, 1, 0, -1, -1)^T. \qquad \square$$

Proof of Proposition 1.2. If n is prime and Equation (1) has rational coefficients, the only way for Equation (1) to have a solution of minimal period n is for $\tau_n^n u[n] = u[n]$ to be a periodic point of Equation (1). If n is prime and greater than 2, we have

$$\Phi_n(x) = x^{n-1} + x^{n-2} + \cdots x + 1.$$

Write

$$v = (0, 1, -1, 1, -1, \ldots, (-1)^n)^T.$$

Any entry of $\Phi_n(S_n)v$ will consist of a zero added to $(n-1)/2$ "1"s and $(n-1)/2$ "-1"s. Thus we see that v is a valid choice for $u[n]$, and the proposition follows. □

Proof of Proposition 1.3. If r is prime the only way for Equation (1) to have a solution of minimal period r is for $\tau_r^n u[r]$ to be a periodic point of Equation (1). In this case we must have $\phi(r) \leq n$. But if $r > n + 1$, then $\phi(r) = r - 1 > n$. □

Remark 4.7. The feature of the rational field $\mathbb{Q}$ that we rely on in this paper is that the cyclotomic polynomials are irreducible over $\mathbb{Q}$. Results analogous to those presented here should hold for equations with coefficients in other subfields of $\mathbb{C}$, at least for particular values of n, depending on how $x^n - 1$ factors over that subfield.

Acknowledgement

I thank the referee for multiple careful readings of drafts of this manuscript. I thank my colleague Dr. Keir Lockridge for the proof of Lemma 2.1 used here.

References

[1] Michael Artin, *Algebra*, Prentice Hall 1991.

[2] Paulo Ney de Souza and Jorge-Nuno Silva, *Berkeley Problems in Mathematics, 3rd edition*, Springer 2004.

[3] Saber Elyadi, *An Introduction to Difference Equations, Third Edition*, Undergraduate Texts in Mathematics, Springer 2008.

[4] Joseph A. Gallian, *Comtemporary Abstract Algebra, 7th edition*, Brooks/Cole 2010.

[5] K.D. Joshi, *Foundations of Discrete Mathematics*, John Wiley and Sons 1989.

[6] Steven Roman, *Advanced Linear Algebra*, Graduate Texts in Mathematics 135, Springer 1992.

Benjamin B. Kennedy
Gettysburg College